



INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume3, Issue3)

Available online at www.ijariit.com

High-Security Data Hiding In Videos Using Multi-Frame, Image Cropping, and LSB Algorithm

Bharathi D. A

SJB Institute of Technology, Bengaluru
bharathida46@gmail.com

Anitha .P

SJB Institute of Technology, Bengaluru
anitha.peram@gmail.com

Kiran S. M

BNM Institute of Technology, Bengaluru
sm.kirana@gmail.com

Abstract: An art of invisible communication by embedding secret information in other sources like text, image, audio, and video is called steganography. A high-security data hiding technique is proposed in this paper. Selected frames from the video are cropped into four equal parts, a block of secret data is hiding in each three channels of the crop of a frame using LSB technique in a predefined sequence, and then image crops are joined to get stego image/ frame. This stego frame is replaced in the video in its original position. A comparative study is performed between proposed approach and existing approach using different metrics such as visualization test, MSE, PSNR and CPU time. Experimental results show that the proposed approach is more secure compared to the existing approach.

Keywords: Steganography, LSB Technique, MSE, PSNR.

I. INTRODUCTION

As the technology improves most of the people started using the internet for exchanging of information. The information may be text, image, audio, video or any type of multimedia. Some information related to banking, army and many government organizations is very secret, but sending such information through the internet is not always safe. The Internet is very weak for data security because many unauthorized viewers can monitor the data on the internet. For secure data transmission through the Internet, a technique called steganography is used. Steganography is a technique of hiding secret message/ information such as text, image or image in another source like image or video, so is not visible to the unauthorized people.

The word steganography came from two Greek words Steganos (secret) and Graphic (writing), it means “secret writing” [1]. There exist different Steganography techniques such as audio steganography, video steganography, text steganography and image steganography. In video steganography, secret information such as text, image, audio or other video frames can be hidden in the video. The cover video in which data is hidden is called stage video. The video contains multiple numbers of images called frames. In video steganography, particular frame from the video is extracted and the secret information is hidden in that frame after information hiding the frame is replaced in its original position in the video.

Generally to increase the security level, before hiding data a technique called cryptography is used. In cryptography the information is changed using a secret key before it is sent, this process of changing text is called “cipher” and the changed text is called “cipher text”. It is very hard to read the changed text. To retrieve the information the person should know the secret key. Only the sender and the receiver should know the secret key from which message can be decrypted.

Various methods are available to hide data in image/video frame. Some of them include image masking and filtering, transformations and least significant bit replacement. In masking and filtering method, luminance part of the color image is modified based on the information content. Since the human eye is less sensitive to luminance component, the visible properties of the color image do not change. Discrete cosine transform (DCT) are used in transformation method and the complexity of this method is more. The complexity of Least Significant Bit (LSB) replacement method is low and it is widely used in steganography.

In LSB, each character in the information is first converted into a string of 8 binary bits. And these 8 bits are replaced with least significant bits of each color of image pixel, in such a way that 3 bits in red, 3 bits in green and 2 bits in blue. Human eye is more sensitive to blue color, hence only 2 bits are modified in blue color.

Intruders always try to access the secret data from the internet. It is a bit easy to access data when the data is hiding in image continuously. To overcome this, a new technique called image cropping is implemented in this paper. In this technique, a frame is extracted from the video and it is treated as a normal RGB image for data hiding. Here image and information are cropped into 4 equal parts and each crop of information is hidden in an image crop. Finally, all image crops containing secret information are joined so that it looks like an original image. Since the information is not continuously hidden in the image, it is difficult to access the data by unauthorized people.

II. LITERATURE SURVEY

Various methods are available to hide data in image/video frame. Some of them include image masking and filtering, transformations and least significant bit replacement. In masking and filtering method, luminance part of the color image is modified based on the information content. Since the human eye is less sensitive to luminance component, the visible properties of the color image do not change. Discrete cosine transform (DCT) are used in transformation method and the complexity of this method is more. The complexity of Least Significant Bit (LSB) replacement method is low and it is widely used in steganography.

In LSB, each character in the information is first converted into a string of 8 binary bits. And these 8 bits are replaced with least significant bits of each color of the image pixel, in such a way that 3 bits in red, 3 bits in green and 2 bits in blue. The human eye is more sensitive to blue color, hence only 2 bits are modified in blue color.

Intruders always try to access the secret data from the internet. It is a bit easy to access data when the data is hiding in image continuously. To overcome this, a new technique called image cropping is implemented in this paper. In this technique, a frame is extracted from the video and it is treated as a normal RGB image for data hiding. Here image and information are cropped into 4 equal parts and each crop of information is hidden in an image crop. Finally, all image crops containing secret information are joined so that it looks like an original image. Since the information is not continuously hidden in the image, it is difficult to access the data by unauthorized people.

Various historical examples say that the technique of data hiding is originated in 440 BC. In the ancient years, human shaved heads were used to hide data, the secret messages were marking on the scalp of the shaved head, ones the hair had grown the person is sending on his way to convey the message [2]. Ancient Greek records describe the use of wax tablets for hiding secret messages. The message is inscribing on the wood, above which a wax is coated, and it looks like a new unused tablet. Resulting tablets could be transported without anyone suspecting the presence of a message beneath the wax [3].

During II world war, Germans use a microdot technology for secret communication. In the recent years, different techniques are developed to hide data in various media such as text, images, audio, and video.

There exist different methods to hide data in image/video frame, some of them includes image masking, transformations, and least significant bit [LSB] methods. LSB is most widely using and simplest technique, here least significant bit of the pixel is replaced with a message bit [4].

A simple image steganography technique is implemented in [5], a secret text message is hidden in 3 channels of RGB image using LSB technique. Yadav, P. et al [6], proposed a technique to hide data in the video. The video is broken into a number of frames, each frame is treated as an individual image. Video Steganography provides more space for secreting the information. Along with Steganography, Cryptography is used in [7], before hiding the data, it is encrypted using a secret key shared between both sender and recipient. At the recipient end encrypted data is first extracted from the image and then it is decrypted using a secret key.

Khalid A. Al-Afandy et. Al [8], proposed high-security data hiding technique in images using image cropping technique. In this technique, before hiding the data the cover image and secret text message are divided into four equal crops. Each crop of text is encrypted using a secret key, then encrypted data is hiding in an image crop using LSB algorithm. Since the information is not continuously hiding in the image, the security of message will be more.

III. PROPOSED APPROACH

The main aim of this proposed technique is to increase the security in video steganography. This approach includes hiding information in multiple frames of video using image cropping and LSB approach. The multiple frames are selected from color video and each frame is divided into four equal parts, an example is shown in fig (2) and fig (3). Here the secret information used is a long string of unformatted text, this string also divided into a number of substrings equal to the number of frame crops. Initially, each character in text is converted into its equivalent decimal number. Later it is encrypted using a secret key (decimal number) \ by the bit-wise EX-OR operation.

Each character of encrypted cipher text is hidden in each pixel of the image using LSB technique. Such that 3 bits of a character in the red channel, 3 bits in the green channel and 2 in the blue channel. After hiding data in image crops, crops are joined to look like original image and finally, the frames are replaced in the video in their original position.

During decryption, the frames having message are selected and cropped each frame into 4 equal parts. The cipher text of secret information hidden in each frame is extracted separately, it is decrypted using bit-wise EX-NOR and then all the information is grouped to get original secret information.

BLOCK DIAGRAM

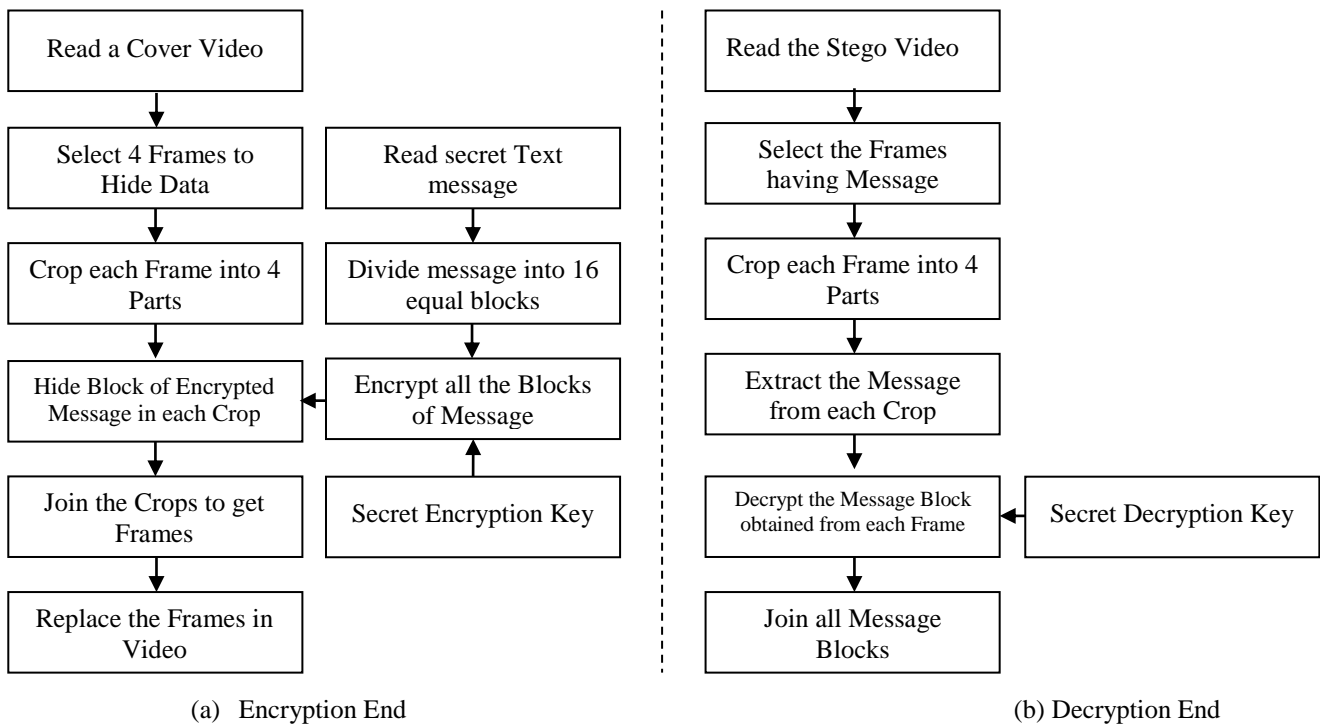


Fig 1: Block diagram of Proposed Approach

LSB ALGORITHM

LSB algorithm is very simple and most widely used in steganography technique. This technique is used to hide text, image, audio as well as video [9]. As the name, LSB says, only least significant bits are used to hide data. For an image with a pixel depth of 8 bits, any changes in two or three least significant bits do not affect much. In this technique before hiding data, each character of a secret message is converted to 8-bit binary sequence. These eight bits are replaced with eight least significant bits of the cover image pixel.

RGB image has three different channels: red, green and blue and each pixel is represented using 24 bits (8 bits for each channel). The information is hidden in all three channels using three bits in red, three bits in green and two bits in blue. The order of hiding the information can be any sequence. Simple example with a sequence of hiding RGBBGRRG (i.e MSB of data is hidden in the red channel, next lower bit in the green channel, and so on) shown below.

Let the original value of an image pixel be: Red-187, Green- 233, and Blue-52.

channel	Red	Green	Blue
Bin Val	10111011	11101001	00110100
Dec Val	187	233	52

If the hiding sequence is 01011101 then after hiding data value of image pixel become:

channel	Red	Green	Blue
Bin Val	10111010	11101111	00110110
Dec Val	186	239	54

Above example clearly indicates the changes in pixel values. Since the changes are very small, human eye cannot identify these minute changes in pixel colour.

At the decoding end bits are accessed from each pixel in the order same as they hide.

IV. RESULTS AND DISCUSSIONS

All tests have been performed using an Intel Core i5 CPU M480 @2.67GHz processor with 4GB RAM, running Windows 8 64-bit operating system and using MATLAB 8.1(R2013a). AVI video of duration 10 seconds is used for simulation. The video contains 240 frames and the size of each frame is 308x640. The secret message to hide is unformatted text document having 4053 characters.

Four frames are selected from the video, each frame is cropped, data is hidden in each crop, crops are rejoined to get ego frame and finally, all stego frames are replaced in the video in their original position. All the results are discussed below are with respect to the single frame (i.e. frame number 23).



Fig 2: Video frame

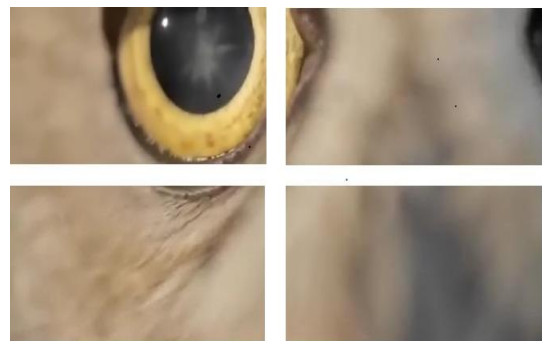


Fig 3: Video frame crops

The performance of the proposed method is measured using four different tests: visual test to determine the degradation in image quality, mean square error, peak signal-to-noise ratio and CPU time.

Visual test results for proposed algorithm and an algorithm for video steganography without image cropping is shown in fig 4. It is clear that variations in the image cannot be identified and there is no degradation in the image quality.


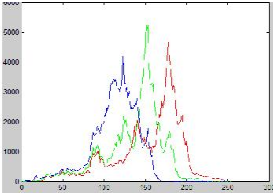

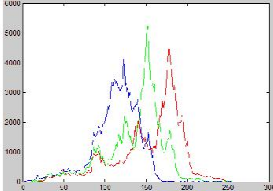

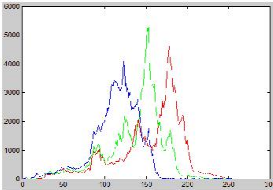
	Image/Frame	Histogram
Original		
Stego image without image cropping		
Stego image with image cropping		

Fig 4: Visual test results

The mean square error (MSE) and peak signal-to-noise ratio (PSNR) are the two error metrics used to compare image compression technique. MSE gives the square error between compressed and original image. PSNR is a measure of peak error. These are mathematically represented as:

$$MSE = \frac{1}{M \times N} \sum_{x=1}^M \sum_{y=1}^N ((I(x,y) - J(x,y))^2) \dots (1)$$

$$PSNR(DB) = 10 \log_{10} \frac{255^2}{MSE} \dots \dots \dots (2)$$

Where M and N represent dimensions of the image, I am compressed image and J represents an original uncompressed image.

The mean square error should be small. Small MSE means that the randomness reflects the data more accurately than a larger MSE. PSNR must be high for best results. MSE, PSNR and CPU time for proposed algorithm with image cropping technique and existing algorithm without image cropping technique are shown in Table I.

From the table, it is clear that MSE of the proposed method is less compared to the existing algorithm. More PSNR indicates the proposed method is better than the existing method. Since all selected frames to be cropped and they should be joined after encrypting, proposed method takes more CPU time than existing.

Table I: MSE, PSNR and CPU time for proposed and existing algorithms

	Proposed algorithm without Image cropping	Existing algorithm with Image cropping
MSE	0.1526	0.0681
PSNR (DB)	57.8744	58.4456
CPU Time	16.5205 (sec)	18.7825 c)

CONCLUSION

This paper proposed a High-security data hiding technique in videos using multi-frame, image cropping, and LSB algorithm. In this work multiple frames are selected from the video, each frame is divided into four crops, a secret information is hiding in each crop. After hiding data crops are joined to get stage image/frame later the frames are replaced in the video in their original position.

From the results, this proves to be a more secure method for data hiding. This technique can be implemented in secrecy departments like military, banking and even in daily life

REFERENCES

1. Amritpal Singh and Harpal Singh, "An Improved LSB based Image Steganography Technique for RGB Images" Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on 5-7 March 2015
2. <https://en.wikipedia.org/wiki/Steganography>
3. Arvind Kumar and K M Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications, Volume 9– No.7, November 2010
4. Rawat, Deepesh, and Vijaya Bhandari., "Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method", International Journal of Computer Applications, Vol. 67, No. 1, PP. 22-25, 2013.
5. Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dung have, "Steganography Using Least Significant Bit Algorithm", International Journal of Engineering Research and Applications (UERA), Vol. 2, Issue 3, pp. 338-34 1,2012.

6. Yadav, P, Sharma, S, Mishra, N, "A secured video steganography along with encryption based on lest significant bit technique", IEEE International Conference on Digital Object Computational Intelligence and Computing Research (ICCIC), 2013 IEEE.
7. Saikia, M, Thakur, V, "Hiding image as the secret message in video", International Conference on Intelligent Systems and Signal Processing (ISSP), 2013.
8. Khalid A. Al-Afandy, El-Sayed M. EL-Rabaie, Osama S. Faragallah, Ahmed ELmhalawy, M. El-Banby, "High-Security Data Hiding Using Image Cropping and LSB Least Significant Bit Steganography" Information Science and Technology (CiSt), 2016 4th IEEE International Colloquium, 24-26 Oct 2016,
9. Manu Devi, Nidhi Sharma, "Improved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images", In Proc. IEEE RAECS UIET Panjab University Chandigarh, March 20 14.